

INTERFERENCE SEARCH

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L3	3	(transmitting environment information collecting processing encrypted secret key).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/04/01 14:55
L5	1	(safety judgment biological environment certificate key public authentication).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/04/01 14:57
L6	2	(biological information peripheral software certificate).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/04/01 14:57
L7	1	(environment transmitting certificate electronic biological).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/04/01 14:58

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L6	2431	environment\$3 same information same software same transmit\$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/01 13:06
L7	120	L6 and certificate and encrypt\$3 and key	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/01 13:06
L8	14	L7 and authenticat\$3 and (biometric or biological)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/01 13:07
L9	9	L8 and @ad<"20021106"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/01 13:07
S1	418	(713/175).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/30 17:08
S2	261	S1 and @ad<"20021106"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/01 12:50
S3	2	("6016479").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/30 17:38
S4	10858	Kotani.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/30 17:39
S5	82	(kotani and seigo).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/30 17:39

EAST Search History

S6	49	S5 and fujitsu	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/30 17:47
S7	1177	713/186	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/30 17:47
S8	720	S7 and @ad<"20021106"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/30 18:28
S9	2575	713/168	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/30 18:28
S10	1820	S9 and @ad<"20021106"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/01 13:07
S11	2621	S10 S8 S2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/30 19:03
S12	81	encrypt\$3 same transmit\$3 same certificate same "secret key" same authentication	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/30 19:04
S13	9	S12 and (biometric or biological)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/01 13:05
S14	3	S13 and @ad<"20021106"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/30 19:10

EAST Search History

S15	2	encrypt\$3 decrypt\$ "public key" certificate enviornment\$3 transmit\$4 authenticat\$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/30 20:10
S16	6	(("6842906") or ("6434561") or ("6289382")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/30 20:11


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)
 The ACM Digital Library The Guide

THE ACM DIGITAL LIBRARY
[Feedback](#) [Report a problem](#) [Satisfaction](#)
Terms used
[biological collect\\$3 enviroment software peripheral authentication](#) [transmit\\$4 encrypt\\$3 decrypt\\$3 certificate](#)

Sort results by
 Save results to a Binder

Try an [Advanced Search](#)

Display results
 Search Tips

Try this search in [The ACM Guide](#)
 Open results in a new window

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

Relevance scale

1 [IS '97: model curriculum and guidelines for undergraduate degree programs in information systems](#)



Gordon B. Davis, John T. Gorgone, J. Daniel Couger, David L. Feinstein, Herbert E. Longenecker
 December 1996 **ACM SIGMIS Database , Guidelines for undergraduate degree programs on Model curriculum and guidelines for undergraduate degree programs in information systems IS '97**, Volume 28 Issue 1

Publisher: ACM Press

 Full text available: [pdf\(7.24 MB\)](#)

 Additional Information: [full citation](#), [citations](#)

2 [Frontmatter \(TOC, Miscellaneous material\)](#)



ACM SIGSOFT Software Engineering Notes staff
 November 2006 **ACM SIGSOFT Software Engineering Notes**, Volume 31 Issue 6

Publisher: ACM Press

 Full text available: [pdf\(1.25 MB\)](#)

 Additional Information: [full citation](#)

3 [Data base directions: the next steps](#)



John L. Berg
 November 1976 **ACM SIGMOD Record , ACM SIGMIS Database**, Volume 8 , 8 Issue 4 , 2

Publisher: ACM Press

 Full text available: [pdf\(9.95 MB\)](#)

 Additional Information: [full citation](#), [abstract](#), [citations](#)

What information about data base technology does a manager need to make prudent decisions using this new technology? To provide this information the National Bureau of Standards and the Association for Computing Machinery established a workshop of approximately 80 experts in five major subject areas. The five subject areas were auditing, evolving technology, government regulations, standards, and user experience. Each area prepared a report contained in these proceedings. The proceedings p ...

Keywords: DBMS, auditing, cost/benefit analysis, data base, data base management, government regulation, management objectives, privacy, security, standards, technology assessment, user experience

Construction engineering and project management: construction simulation methodologies Eucalyptus: intelligent infrastructure enabled participatory design studio

Michael Jemtrud, Philam Nguyen, Bruce Spencer, Martin Brooks, Sandy Liu, Yong Liang, Bo Xu, Lib Zhang

December 2006 **Proceedings of the 37th conference on Winter simulation WSC '06**

Publisher: Winter Simulation Conference

Full text available: [pdf\(240.91 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

A new notion of participation is at stake with advances in technologically mediated work environments. Insufficient bandwidth and insufficiently powerful, crudely coordinated tools result in distributed task-based modes of collaboration that did not allow full participation by members of distributed design teams. The emergence of Service Oriented Architectures (SOA) and User-Computer Light-Paths (UCLP) herald the beginning of a new age where fully participatory multi-site design become possible ...

5 Implementing role based access control for federated information systems on the web

Kerry Taylor, James Murty

January 2003 **Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003 - Volume 21 ACSW Frontiers '03**

Publisher: Australian Computer Society, Inc.

Full text available: [pdf\(217.89 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index term](#)

There is rapidly increasing interest in Australia in on-line sharing of information stored in corporate databases, especially within and between staff of independent government agencies. Biological collections databases and population health GIS are good examples of the frequent situation where database custodians are looking for dynamic, distributed, heterogeneous federated information systems models for information sharing within loosely constituted communities. This paper describes a system ...

Keywords: RBAC, federated databases

6 Terra: a virtual machine-based platform for trusted computing

 Tal Garfinkel, Ben Pfaff, Jim Chow, Mendel Rosenblum, Dan Boneh

October 2003 **ACM SIGOPS Operating Systems Review , Proceedings of the nineteenth ACM symposium on Operating systems principles SOSP '03**, Volume 37 Issue 5

Publisher: ACM Press

Full text available: [pdf\(140.31 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index term](#)

We present a flexible architecture for trusted computing, called Terra, that allows applications with a wide range of security requirements to run simultaneously on commodity hardware. Applications running on Terra enjoy the semantics of running on a separate, dedicated, tamper-resistant hardware platform while retaining the ability to run side-by-side with normal applications on a general-purpose computing platform. Terra achieves this synthesis by use of a *trusted virtual machine monitor* (TVMM) ...

Keywords: VMM, attestation, authentication, trusted computing, virtual machine, virtual machine monitor

7 Virtual extension: Authentication in e-commerce

 Amit Basu, Steve Muyllle

December 2003 **Communications of the ACM**, Volume 46 Issue 12

Publisher: ACM Press

Full text available: [pdf\(282.22 KB\)](#) [html\(30.40 KB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

8 Frontmatter (TOC, Letters, Election results, Software Reliability Resources!, Computing Curricula 2004 and the Software Engineering Volume SE2004, Software Reuse Research, 2005 Forward)

July 2005 **ACM SIGSOFT Software Engineering Notes**, Volume 30 Issue 4

Publisher: ACM Press

Full text available: [!\[\]\(9dfdaff1d86ba3c1f8353b4d1b61b8c5_img.jpg\) pdf\(6.19 MB\)](#)

Additional Information: [full citation](#), [index terms](#)

9 Identity verification (authentication) working group

Tom Berson, P. Capek, J. Schweitzer, C. Weissman

April 1988 **ACM SIGSAC Review**, Volume 6 Issue 1

Publisher: ACM Press

Full text available: [!\[\]\(d0262bbe9d2356661a2e89321dfcc781_img.jpg\) pdf\(803.95 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [index terms](#)

Every reader of this report has at some time verified his or her identity to a computer system. The use of a userid and password in response to computer prompting is the almost universal model for this simple but essential act.

10 Session 4 (full technical papers): evolution patterns and models: Evolution patterns of open source software systems and communities

Kumiyo Nakakoji, Yasuhiro Yamamoto, Yoshiyuki Nishinaka, Kouichi Kishida, Yunwen Ye

May 2002 **Proceedings of the International Workshop on Principles of Software Evolution: IWPSE '02**

Publisher: ACM Press

Full text available: [!\[\]\(683dba75afe26e28cd4de5730b776760_img.jpg\) pdf\(1.06 MB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

Open-Source Software (OSS) development is regarded as a successful model of encouraging "natural product evolution". To understand how this "natural product evolution" happens, we have conducted a case study of four typical OSS projects. Unlike most previous studies on software evolution that focus on the evolution of the system per se, our study takes a broader perspective: It examines not only the evolution of OSS systems, but also the evolution of the associated OSS communities, as well as ...

Keywords: case study, open-source software (OSS), open-source software community, software evolution

11 Security in embedded systems: Design challenges

Srivaths Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady

August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3

Publisher: ACM Press

Full text available: [!\[\]\(6b6d798a1e19654494a6892c667d44da_img.jpg\) pdf\(3.67 MB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

Many modern electronic systems---including personal computers, PDAs, cell phones, network routers, smart cards, and networked sensors to name a few---need to access, store, manipulate, or communicate sensitive information, making security a serious concern in their design. Embedded systems, which account for a wide range of products from the electronics, semiconductor, telecommunications, and networking industries, face some of the most demanding security constraints on the one hand, they are often ...

Keywords: Embedded systems, architecture, authentication, battery life, cryptographic algorithms, decryption, encryption, hardware design, processing requirements, security, security attacks, se

protocols, tamper resistance

12 A survey of autonomic communications

 Simon Dobson, Spyros Denazis, Antonio Fernández, Dominique Gaïti, Erol Gelenbe, Fabio Massacci
Paddy Nixon, Fabrice Saffre, Nikita Schmidt, Franco Zambonelli

December 2006 **ACM Transactions on Autonomous and Adaptive Systems (TAAS)**, Volume 1 Is:

Publisher: ACM Press

Full text available:  pdf(300.86 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Autonomic communications seek to improve the ability of network and services to cope with unpredicted change, including changes in topology, load, task, the physical and logical character of the networks that can be accessed, and so forth. Broad-ranging autonomic solutions require designers to account for a range of end-to-end issues affecting programming models, network and contextual modeling and reasoning, decentralised algorithms, trust acquisition and maintenance issues whose soluti ...

Keywords: Autonomic communication

13 Practice: Cybercrime, identity theft, and fraud: practicing safe internet - network security threats and vulnerabilities

 Robert C. Newman
September 2006 **Proceedings of the 3rd annual conference on Information security curricul development InfoSecCD '06**

Publisher: ACM Press

Full text available:  pdf(123.56 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Computer networks and computer systems are experiencing attacks and threats from many are Threats are also extended to include the individual user's computer assets and resources. Infor will be presented on the categories of security and privacy threats, integrity threats, vulnerability delay and denial threats, and intellectual property threats that are being directed towards corp educational, governmental, and individual assets.

Keywords: cybercrime, identity theft, internet fraud

14 Open source and distributed software development: Seeking the source: software source code as a social and technical artifact

 Cleidson de Souza, Jon Froehlich, Paul Dourish
November 2005 **Proceedings of the 2005 international ACM SIGGROUP conference on Supporting group work GROUP '05**

Publisher: ACM Press

Full text available:  pdf(1.57 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

In distributed software development, two sorts of dependencies can arise. The structure of the software system itself can create dependencies between software elements, while the structure development process can create dependencies between software developers. Each of these both shapes and reflects the development process. Our research concerns the extent to which, by looking uniformly at artifacts and activities, we can uncover the structures of software projects, and the in which ...

Keywords: data mining, social networks, socio-technical systems, software repositories

15 Applications and system issues: Securing user inputs for the web

 Jan Camenisch, Dieter Sommer, Roger Zimmermann

November 2006 **Proceedings of the second ACM workshop on Digital identity management '06**

Publisher: ACM Press

Full text available:  pdf(655.02 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The goal of this paper is to study *secure and usable* methods for providing user input to a web site. Three principles define security for us: certification, awareness, and privacy. Four principles define usability: contextual awareness, semantic awareness, prodigious use of screen space, and the availability of recommended choices. We first describe how current approaches to the solicitation of user input on the web fail on both fronts: they either can not handle certified data, do not resp

Keywords: user interface designs

16 DIM security and authentication: Authentication using multiple communication channels

 Shintaro Mizuno, Kohji Yamada, Kenji Takahashi

November 2005 **Proceedings of the 2005 workshop on Digital identity management DIM '05**

Publisher: ACM Press

Full text available:  pdf(3.02 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We discuss an authentication method using multiple communication channels. This method enables on-line service providers to strongly authenticate their users on a non-trusted communication channel (e.g. using a kiosk PC in an Internet café to access the Internet) via trusted communication channels (e.g. a mobile phone network). For the illustration purpose, we use a commonly available configuration in the current marketplace, in which users access service providers through PCs on the Internet ...

Keywords: authentication, internet, mobile phone, multiple channels

17 SafeBots: a paradigm for software security controls

 Robert Filman, Ted Linden

September 1996 **Proceedings of the 1996 workshop on New security paradigms NSPW '96**

Publisher: ACM Press

Full text available:  pdf(754.67 KB)

Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

18 Invited papers on the frontiers of software practice: Cybersecurity

Richard A. Kemmerer

May 2003 **Proceedings of the 25th International Conference on Software Engineering ICSE '03**

Publisher: IEEE Computer Society

Full text available:  pdf(1.17 MB) 

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)
[Publisher Site](#)

As more business activities are being automated and an increasing number of computers are being used to store sensitive information, the need for secure computer systems becomes more apparent. This need is even more apparent as systems and applications are being distributed and accessed over an insecure network, such as the Internet. The Internet itself has become critical for governments, companies, financial institutions, and millions of everyday users. Networks of computers support a multitude ...

19 Trusted paths for browsers

Zishuang (Eileen) Ye, Sean Smith, Denise Anthony

 May 2005 **ACM Transactions on Information and System Security (TISSEC)**, Volume 8 Issue 2
Publisher: ACM Press
Full text available: [pdf\(265.37 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index term](#):

Computer security protocols usually terminate in a computer; however, the human-based services which they support usually terminate in a human. The gap between the human and the computer creates potential for security problems. We examine this gap, as it is manifested in secure Web servers. Felten et al. demonstrated the potential, in 1996, for malicious servers to impersonate honest servers. In this paper, we show how malicious servers can still do this---and can also force the existence of an ...

Keywords: HCISEC, Trust path, Web browser security

20 [Processor microarchitecture II: AEGIS: architecture for tamper-evident and tamper-resistant processing](#)

 G. Edward Suh, Dwaine Clarke, Blaise Gassend, Marten van Dijk, Srinivas Devadas
June 2003 **Proceedings of the 17th annual international conference on Supercomputing I '03**

Publisher: ACM Press

Full text available: [pdf\(286.90 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index term](#):

We describe the architecture for a single-chip aegis processor which can be used to build computer systems secure against both physical and software attacks. Our architecture assumes that all components external to the processor, such as memory, are untrusted. We show two different implementations. In the first case, the core functionality of the operating system is trusted and implemented in a security kernel. We also describe a variant implementation assuming an untrusted operating system ...

Keywords: certified execution, secure processors, software licensing

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.
[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads: [Adobe Acrobat](#) [QuickTime](#) [Windows Media Player](#) [Real Player](#)